



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,816	10/25/2001	Benjamin J. Parker	1688 (15723)	4720

33272 7590 09/26/2006

SPRINT COMMUNICATIONS COMPANY L.P.
6391 SPRINT PARKWAY
MAILSTOP: KSOPHT0101-Z2100
OVERLAND PARK, KS 66251-2100

EXAMINER

COLIN, CARL G

ART UNIT PAPER NUMBER

2136

DATE MAILED: 09/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/003,816	Applicant(s) PARKER ET AL.	
	Examiner Carl Colin	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 11 July 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. In response to communications filed on 7/11/2006, the following claims 1-20 are presented for examination.

2. Applicant's arguments filed 7/11/2006 with respect to claims 1-20 have been fully considered but they are not persuasive. Applicant argues that Wadlow et al fails to disclose "security service pathways, each providing a respective combination of security features".

Examiner asserts that the citations provided by the Examiner do disclose the claimed limitation as claimed and Applicant fails to explain how they do not. Wadlow even claims the above limitation in claim 1 of Wadlow's reference:

"a plurality of packet processing components;
a plurality of communication paths between components of the plurality of packet processing components; and
configurable policy enforcement means, at each connection of a communication path and a packet processing component, for enforcing a packet policy for packets transported between the communication path and the packet processing component, wherein the packet policy is a function of the customer security policies."

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., upon directing to a pathway by the service selection gateway, no further routing between the security devices is necessary with the present invention) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Wadlow to include the concept of Barrett and implement user configurable setting allowing user to specify conditions for blocking or allowing any type of communication or access with outside computers and devices. One of ordinary skill in the art would have been motivated to do so because it would provide a security solution that doesn't impose one-size-fits-all solution on the users of the network (Col 5, Lines 5-21) and a user changeable security setting that would specify which outside computers and network devices may access a user computer and what type of access to the user computer is allowed (Col 5, lines 50-62) as disclosed below in the Office Action. Therefore, claims 1-20 remain rejected.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have

Art Unit: 2136

been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-2, 4-5, 9-14, and 16-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wadlow et al.** US (6,230,271) in view of **Barrett** US (6,832,321).

As per claim 1: Wadlow discloses a private network apparatus for connecting a user to an external Internet comprising: A plurality of security service pathways each providing a respective combination of security service features; (Col 2, lines 40-46 and Col 3, line 56 through column 4, line 16 and claim 1); discloses policy application allowing user to configure security features for user traffic that meets the recitation of a service selection dashboard allowing said user to select from a plurality of security service features for user traffic to and from said user (Col 6, line 37 through Col 7, line 12 and Col 8, Lines 45-67); Col 7-8 provide more detailed explanation; Also, Col 4; lines 32-58 and item MW in Figure 1 discloses a Maintenance Workstation used to inspect or change the behavior of devices); a network management server coupled to said service selection dashboard for storing a subscriber configuration in response to said user selected security service features (Col 8, Lines 45-67); a maintenance router or CSR or CLR that meets the recitation of a pass-through router for coupling to said user traffic to said external internet independently of said security service pathways (Col 4, lines 36-44), (see also application level proxy embodiment Col 8, lines 40-45); a service selection gateway coupled to said user for directing said user traffic to and from one of

Art Unit: 2136

said service selection dashboard, said pass-through router, or one of said security service pathways; and (Col 4, lines 30-32 and Col 9, lines 1-35 and Col 9, lines 58-65); an External router that meets the recitation of security service router for coupling said security service pathways to said external Internet; (Col 4, lines 35-44)

- Wherein said service selection gateway directs said user traffic to said service selection dashboard if said subscriber configuration is in an initialized state; (Col 8, Lines 52-56)
- Wherein said service selection gateway directs said user traffic to a respective one of said security service pathways or to said pass-through router in response to said subscriber configuration after initialization by said service selection dashboard. (Col 8, Lines 52-56 and Col 9-10 show different communication pathways between a customer workstation and the public network in response to different security configuration by the customer).

Wadlow discloses a plurality of security service pathways for a user to connect to the Internet according to a plurality of security features. Wadlow does not explicitly disclose identical architecture but it is suggested that different pathways can be established to apply filtering policy between a router and a network interface as well as applications level filtering between the source and destination networks as shown in figs. 4-5 and Col 7, line 48 through Col 8). Barrett teaches the use of a firewall for providing different grades of firewall protection (FIG. 6 and Col 8 lines 25-50) and further teaches that user has the ability to select and specify certain types of connection including a default security setting that is automatically select in the event no security setting is explicitly selecting. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Wadlow to include the concept of Barrett and implement user configurable setting allowing user to specify conditions for blocking or

Art Unit: 2136

allowing any type of communication or access with outside computers and devices. One of ordinary skill in the art would have been motivated to do so because it would provide a security solution that doesn't impose one-size-fits-all solution on the users of the network (Col 5, Lines 5-21) and a user changeable security setting that would specify which outside computers and network devices may access a user computer and what type of access to the user computer is allowed (Col 5, lines 50-62).

As per claim 2: Wadlow discloses the apparatus of claim 1 and a router with a filtering policy that meets the recitation of a firewall wherein said security service pathways include at least one pathway having a firewall. (Col 6, Lines 59-64 and Col 8, lines 11-44).

As per claim 4: Wadlow discloses the apparatus of claim 1 wherein said security service pathways include at least one pathway having a content filter. (Col 8, Lines 12-26)

As per claim 5: Wadlow discloses the apparatus of claim 1 wherein said security service pathways include at least one pathway having a firewall and a content filter. (Col 9, lines 59-64; shows a modification to a packet-filtering path to enable application and packet filtering).

As per claim 9: Barrett discloses using of a firewall providing different grades of firewall protection (FIG. 6 and Col 8 lines 25-50). Therefore, this claim is rejected on the same rationale as the rejection of claim 1 above.

Art Unit: 2136

As per claim 10: Barrett discloses using of a firewall providing high firewall protection (Col 9, Lines 16-21 and Col 8, Lines 27-35 and Col 4, lines 1-7), medium firewall protection (Col 9, Lines 16-21 and Col 8, Lines 27-35) and low firewall protection (Col 9, Lines 16-21).

Therefore, this claim is rejected on the same rationale as the rejection of claim 1 above.

As per claim 11: Barrett discloses using of firewall providing low grade protection by blocking outgoing traffic (Col 9, Lines 16-21). Therefore, this claim is rejected on the same rationale as the rejection of claim 1 above.

As per claim 12: Barrett discloses using of firewall providing medium grade protection by blocking outgoing and incoming traffic (Col 9, Lines 16-21 and Col 8, Lines 27-35). Therefore, this claim is rejected on the same rationale as the rejection of claim 1 above.

As per claim 13: Barrett discloses using of firewall providing medium grade protection by blocking outgoing and incoming traffic not initiated by user (Col 8, Lines 27-35 and Col 4, lines 1-7). Therefore, this claim is rejected on the same rationale as the rejection of claim 1 above.

As per claim 14: Wadlow discloses determining from said subscription profile which security service features to apply to said user traffic; (Col 8); if said subscription profile for said user includes any security service features, then redirecting said user traffic to a particular security service pathway of a plurality of security service pathways, said particular security service pathway corresponding to said security service features identified by said user profile; and if said

Art Unit: 2136

subscription profile for said user includes no security service features, then redirecting said user traffic to a pass-through router for coupling said user traffic to said external internet. Wadlow is silent about directing a user to a captive portal; (Col 8, lines 25-49) presenting security service features to said user Barrett also discloses a method of providing security service in a network interface to an external Internet, said method comprising the steps of: Directing a user to a captive portal; (Col 8, lines 25-49) Presenting security service features to said user; (Col 8; lines 25-49 and FIG. 6) Storing a subscription profile for said user in response to security service features selected by said user through said captive portal; (Col 8, Lines 19-24 and Col 10, lines 23-29) Receiving user traffic from said user destined for said external Internet at a service selection gateway; (Col 8, lines 59-66) Determining from said subscription profile which security service features to apply to said user traffic; (Col 9, Lines 16-21) If said subscription profile for said user includes any security service features, then redirecting said user traffic to a particular security service pathway of a plurality of security service pathways, said particular security service pathway corresponding to said security service features identified by said user profile (Col 7, line 44 through Col 7); and If said subscription profile for said user includes no security service features, then redirecting said user traffic to a pass-through router for coupling said user traffic to said external internet. (Col 9 line 55 through Col 10 line 8). Although not explicitly mention a pass-through router, it is obvious to one of ordinary skill in the art that a router can be placed between the server and each network interface as disclosed in Waldow. Therefore, claim 14 is rejected on the same rationale as the rejection of claim 1.

Art Unit: 2136

As per claim 16: Barrett discloses the method of claim 15 wherein said firewall services comprise selectable grades of firewall protection including a high grade firewall protection, a medium grade firewall protection, and a low grade firewall protection. (FIG. 6 and Col 8 lines 25-50). Therefore, this claim is rejected on the same rationale as the rejection of claim 1 above.

As per claims 17-19: these claims disclose the same limitations as claims 11-13. Therefore, these claims are rejected on the same rationale as the rejection of claims 11-13 above.

As per claim 20: Wadlow discloses the apparatus of claim 1 further comprising: a user-side switch coupling said service selection gateway to said security service pathways (Col 4, Mines 44-51 & CSR in FIG 1); and an internet-side switch coupling said security service pathways to said security service router (Col 4, lines 28-43 & ETC, ER in FIG 1).

4. **Claims 3, 6-7, 8, and 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wadlow et al.** US (6,230,271) in view of **Barrett** US (6,832,321) as applied to claim 1 above and further in view of **Schneider et al.** US (6,178,505).

As per claim 3: Wadlow discloses a plurality of security service pathways including a combination of firewall and application filleting but doesn't explicitly show security service pathways with a virus scanner. However Schneider teaches the using of antivirus system in a network apparatus to provide further protection to users data (Col 42, Lines 10-29). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to

Art Unit: 2136

modify Wadlow system with the teaching of Schneider to include virus scanners on the security pathways. One of ordinary skill in the art would have been motivated to do so in order to provide an additional level of security to the user by ensuring that the transmitted information came from authorized source and doesn't contain any viruses.

As per claim 6: Schneider teaches the using of antivirus system in a network apparatus to provide further protection to users data (Col 42, Lines 10-29). Therefore, this claim is rejected on the same rationale as the rejection of claim 3 above.

As per claim 7: Schneider teaches the using of anti-virus and (Col 42, Lines 10-29) and a content filter system (Col 40, Line 42 through Col 41, Line 29) in a network apparatus to provide protection to users data. Therefore, this claim is rejected on the same rationale as the rejection of claim 3 above.

As per claim 8: Schneider teaches the using of anti-virus and (Col 42, Lines 10-29) and a content filter system (Col 40, Line 42 through Col 41, Line 29) in a network apparatus to provide protection to users data. Therefore, this claim is rejected on the same rationale as the rejection of claim 3 above.

As per claim 15: Schneider teaches the using of anti-virus and (Col 42, Lines 10-29) and a content filter system (Col 40, Line 42 through Col 41, Line 29) in a network apparatus to provide

protection for users. Therefore, this claim is rejected on the same rationale as the rejection of claim 3 above.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2136

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

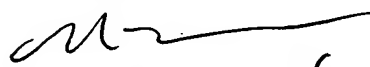
cc

Carl Colin

Patent Examiner

September 19, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


9, 20, 06